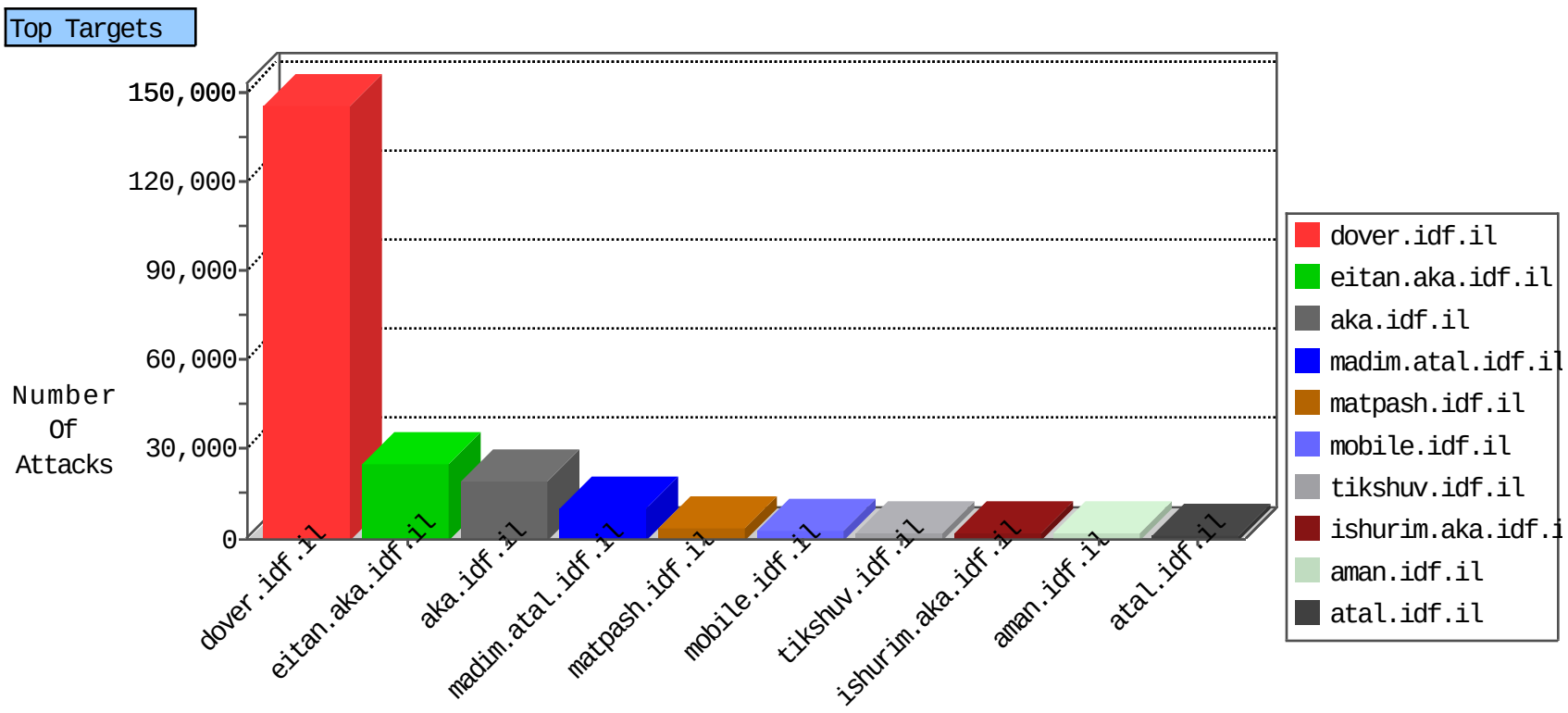
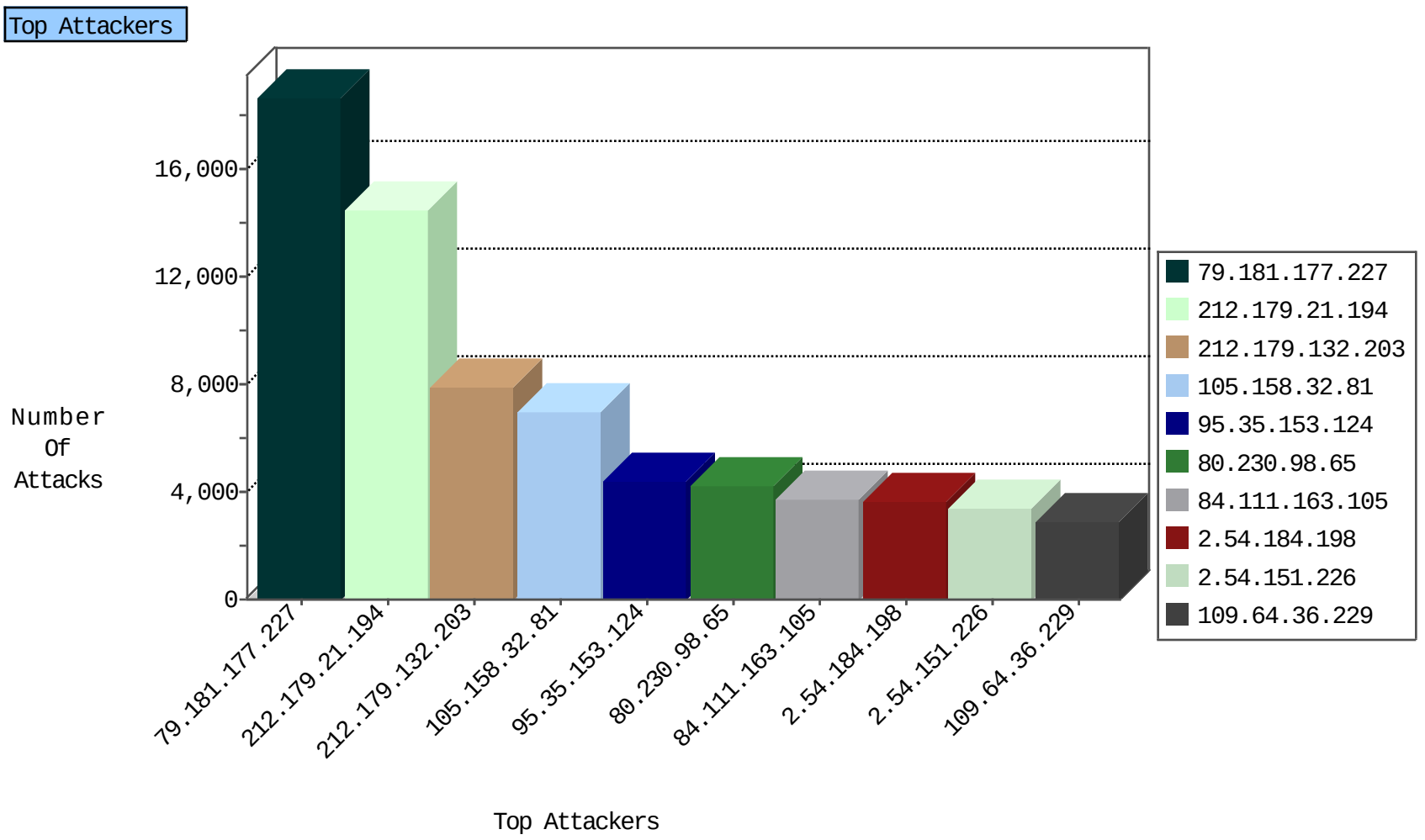
10-27-2015 to 10-28-2015

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-27-2015 to 10-28-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.166	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10017
149.78.154.69	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6328
74.215.76.204	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6037
85.64.191.144	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5701
212.179.21.194	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5694
212.156.70.118	Turkey	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3372
46.19.86.109	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2753
192.198.151.37	Europe	147.237.72.167	ishurim.aka.idf.il	TCP handshake violation, first packet not syn	drop	2349
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	2311
66.249.78.254	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2232
66.249.67.227	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	1311
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	796
52.23.156.32	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	564
79.180.18.248	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	502
176.12.150.20	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	321
89.138.250.190	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	310
93.172.186.1	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	309
66.249.67.219	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	265
41.142.26.6	Morocco	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	255
199.58.81.144	Canada	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	255
80.246.136.56	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	245
185.32.179.215	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	200
66.249.67.235	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	172
80.246.136.9	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	162
220.181.108.77	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	154
168.235.194.228	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	146
66.249.64.146	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	128
212.25.84.200	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	127
46.19.86.121	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	123
46.19.86.67	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	114
207.232.36.181	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	112
217.41.11.42	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	105
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
37.26.148.243	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	93
81.218.241.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	84
46.19.86.82	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	77
2.54.131.46	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	75
46.19.86.198	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	70
176.13.15.156	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	68
2.54.32.103	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	68
37.26.147.242	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	68
2.54.186.56	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	63
80.246.139.175	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	63
2.54.146.196	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	56
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	53
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	51
10.0.0.3		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	51
2.52.7.184	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	50
212.179.159.253	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	45
37.26.147.219	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	45

10-27-2015 to 10-28-2015

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
98.19.222.133	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	60
104.203.59.254	United States	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
104.203.59.254	United States	147.237.77.176	matpash.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
104.203.59.254	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	34
103.21.58.191	India	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	20
104.203.59.254	United States	147.237.77.176	matpash.idf.il	0854: HTTP: upload* Access	Block	12
104.203.59.254	United States	147.237.77.74	law.idf.il	0854: HTTP: upload* Access	Block	12
212.29.202.206	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
104.203.59.254	United States	147.237.77.216	dover.idf.il	0854: HTTP: upload* Access	Block	11
93.172.186.255	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	8
64.186.146.196	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
199.58.81.144	Canada	147.237.77.216	dover.idf.il	10725: TCP: LOIC DDoS Tool	Block	5
87.69.152.189	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
84.109.214.160	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
46.121.228.158	Israel	147.237.77.216	dover.idf.il	C1000098: Block - dns poisoning	Block	3
195.200.205.2	Israel	147.237.76.147	chinuch.aka.idf.il	C1000122: HTTP: Access to - .exe or .dll	Permit	3
46.117.219.208	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
74.208.66.220	United States	147.237.76.31	nakchal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	2
62.90.255.56	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
41.105.127.249	Algeria	147.237.77.216	dover.idf.il	12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	2
209.15.196.171	Canada	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	2
173.201.196.172	United States	147.237.72.166	aka.idf.il	3593: HTTP: SQL Injection (UNION)	Block	2
52.1.90.117	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	2
62.90.96.102	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
24.156.108.59	United States	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
94.29.124.83	Russian Federation	147.237.77.216	dover.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1
173.201.196.161	United States	147.237.72.166	aka.idf.il	3593: HTTP: SQL Injection (UNION)	Block	1
104.203.59.254	United States	147.237.77.74	law.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
212.129.31.161	France	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
188.121.41.45	Netherlands	147.237.72.166	aka.idf.il	3593: HTTP: SQL Injection (UNION)	Block	1
74.208.66.220	United States	147.237.76.31	nakchal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
46.252.205.141	Netherlands	147.237.72.166	aka.idf.il	3593: HTTP: SQL Injection (UNION)	Block	1
89.19.29.90	Turkey	147.237.76.86	navy.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1
188.138.17.205	France	147.237.76.176	test.ncore.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
45.79.109.226		147.237.72.166	aka.idf.il	3624: HTTP: SQL Injection (SELECT)	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
101.108.30.10	Thailand	147.237.77.216	dover.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1
77.126.195.146	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
209.15.196.171	Canada	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
179.7.78.2	Peru	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
50.62.161.232	United States	147.237.72.166	aka.idf.il	3593: HTTP: SQL Injection (UNION)	Block	1
89.19.29.90	Turkey	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
64.186.146.196	United States	147.237.77.74	law.idf.il	3809: HTTP: SQL Injection Evasion SQL Comment Terminator	Block	1
45.79.109.226		147.237.72.167	ishurim.aka.idf.il	3624: HTTP: SQL Injection (SELECT)	Block	1
162.210.196.97	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
82.158.30.199	Spain	147.237.77.176	matpash.idf.il	C008: HTTP: Xenu UserAgent	Block	1
209.58.178.49	United States	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
184.168.152.170	United States	147.237.72.166	aka.idf.il	3593: HTTP: SQL Injection (UNION)	Block	1
66.194.11.113	United States	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
198.71.228.36	United States	147.237.72.166	aka.idf.il	3593: HTTP: SQL Injection (UNION)	Block	1

10-27-2015 to 10-28-2015

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
98.19.222.133	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	153
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	58
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	24
64.186.146.196	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
98.19.222.133	147.237.77.233	United States	atal.idf.il	ET WEB_SERVER SQLi - SELECT and sysobject	6
98.19.222.133	147.237.77.233	United States	atal.idf.il	ET WEB_SERVER ATTACKER SQLi - SELECT and Schema Columns	6
66.249.78.173	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	4
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	3
46.19.85.99	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
46.117.245.208	147.237.77.216	Israel	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
66.249.93.220	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
195.200.205.2	147.237.76.147	Israel	chinuch.aka.idf.il	WEB-FRONTPAGE /_vti_bin/ access	2
176.12.136.15	147.237.76.42	Israel	refuah.idf.il	GPL SCAN myscan	2
195.117.135.75	147.237.77.205	Poland	prisha.idf.il	ET SCAN Potential SSH Scan	2
54.209.60.63	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
5.160.170.106	147.237.76.86	Iran, Islamic Republic of	navy.idf.il	ET SCAN Potential SSH Scan	2
176.12.136.15	147.237.76.42	Israel	refuah.idf.il	INDICATOR-SCAN myscan	2
46.19.85.120	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
171.249.220.240	147.237.76.38	Vietnam	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
103.243.138.30	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
84.108.0.15	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
58.63.239.135	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
194.90.144.146	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
12.216.138.71	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
115.182.17.13	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
93.174.95.77	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
77.202.11.135	147.237.76.38	France	e.e.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
212.7.209.9	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
79.182.118.95	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.235.68.170	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.121.247.46	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.103	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.194.192	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.160.169.242	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.138.196.24	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.102.8.173	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
195.117.135.75	147.237.77.226	Poland	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
37.26.147.161	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
119.254.103.15	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
101.231.154.154	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
103.232.35.93	147.237.72.167	Hong Kong	ishurim.aka.idf.il	ET SCAN NMAP -sS window 3072	1
84.94.66.97	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
58.63.239.135	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
193.201.224.8	147.237.72.166	Ukraine	aka.idf.il	SERVER-WEBAPP admin.php access	1
5.160.170.106	147.237.77.226	Iran, Islamic Republic of	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
115.182.17.13	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -f -sS	1
93.174.93.138	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
77.158.88.41	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
212.7.209.9	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
169.57.5.20	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1

10-27-2015 to 10-28-2015

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14205
212.179.132.203	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7876
105.158.32.81	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6185
95.35.153.124	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4379
80.230.98.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4184
79.181.177.227	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3708
2.54.184.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3609
5.29.79.89	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2766
41.142.26.6	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2156
93.184.3.73	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2091
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1824
80.178.158.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1717
95.35.167.154	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1686
109.67.35.147	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1335
46.163.68.109	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1308
149.78.103.229	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1193
212.179.42.225	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1193
95.35.68.192	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1141
2.54.11.19	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1056
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	863
2.54.182.202	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	806
109.64.36.229	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	774
84.95.252.17	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	765
212.76.101.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	759
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	753
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	726
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	717
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	713
176.106.46.249	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	649
209.88.198.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	616
95.35.177.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	585
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	580
81.218.205.183	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	570
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	538
2.54.10.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	529
2.54.187.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	519
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	507
92.229.17.127	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	497
85.132.24.46	Azerbaijan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	442
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	441
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	437
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	436
37.60.44.80	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	413
77.125.10.75	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	406
79.180.151.209	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	381
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	380
95.35.85.179	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	376
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	367
94.249.61.146	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	351
37.26.149.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	339

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.181.177.227	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	14976
84.111.163.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3725
2.54.151.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3415
109.64.36.229	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 109.64.36.229	Block	2086
192.116.232.69	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	1858
176.13.20.224	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.20.224	Block	1421
81.218.205.183	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 81.218.205.183	Block	1148
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	895
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	840
46.19.86.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	777
213.8.67.71	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.8.67.71	Block	756
105.158.32.81	Morocco	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 105.158.32.81	Block	749
149.78.93.21	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 149.78.93.21	Block	630
46.19.85.1	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.1	Block	490
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	490
104.203.59.254	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 104.203.59.254	Block	406
104.203.59.254	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 104.203.59.254	Block	350
104.203.59.254	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 104.203.59.254	Block	329
37.26.146.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	308
95.35.204.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	308
79.180.151.209	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	307
109.65.158.174	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	224
109.65.158.174	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	224
5.28.131.167	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 5.28.131.167	Block	209
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	196
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	168
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1934-he/cogat.aspx	Block	168
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	154
46.19.85.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	154
2.52.11.250	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	148
77.127.147.244	Israel	147.237.0.17	m.my-kosher-kravi .idf.il	Distributed Illegal Parameter Encoding	None	147
46.19.86.199	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.199	Block	140
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	140
91.200.12.49	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	126
84.109.176.71	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	126
91.200.12.49	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	126
84.109.176.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	126
46.19.85.31	Israel	147.237.76.39	mobile.meitav.idf.il	Cookie Tampering on cookie .ASPNETAUTH: Expected 01022617FBD451DED208FE268F3CA054DED2080009330031003800310036003700350031003700000012F00FF, Observed 0102CAFE5A3E8FDCD208FECA769C0992DCD2080009330031003800310036003700350031003700000012F00FF	None	126
176.12.148.129	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication/index	Block	126
84.108.70.140	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	112
84.108.70.140	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	112
46.19.86.94	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	98
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	98
79.176.216.131	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	98
213.57.206.174	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	98
31.154.135.45	Israel	147.237.77.176	matpash.idf.il	Parameter Type Violation SearchText in www.cogat.idf.il/938-en/cogat.aspx	Block	98
79.176.216.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	98
2.52.133.69	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	98
46.120.95.131	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	98
68.180.228.112	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	96